Galileo Safety & Dependability Programme for Safety-of-Life Applications

TRISMAC CONFERENCE 16th April 2008

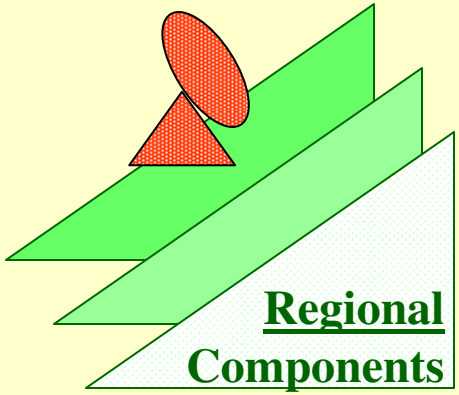
Presentation by:

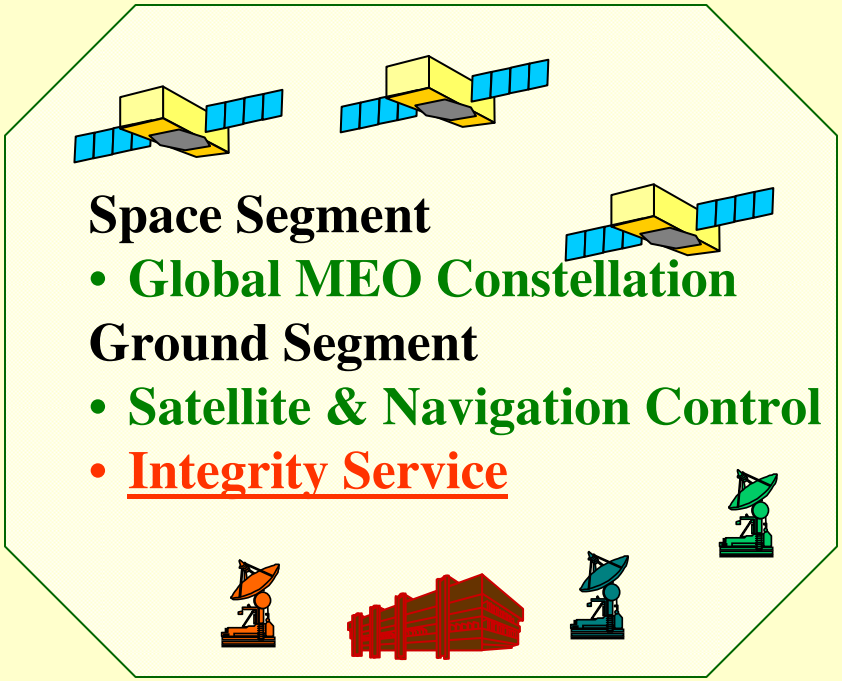
Nigel Watts

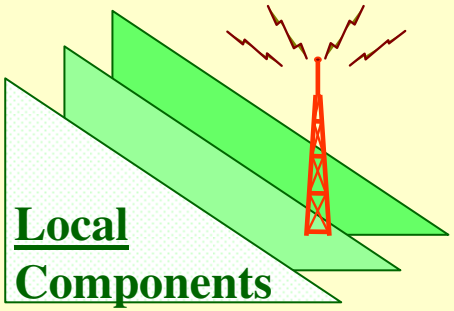
Head of Galileo Product Assurance and Safety Office

(on behalf of Andrew Brown, Galileo RAMS and Certification Manager)

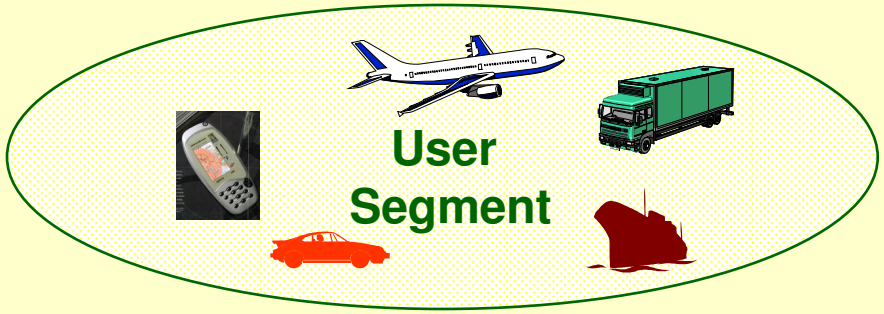
Galileo System

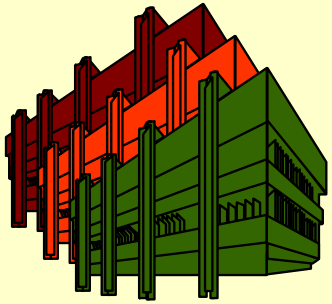






SAR





Service
Centres

Challenges

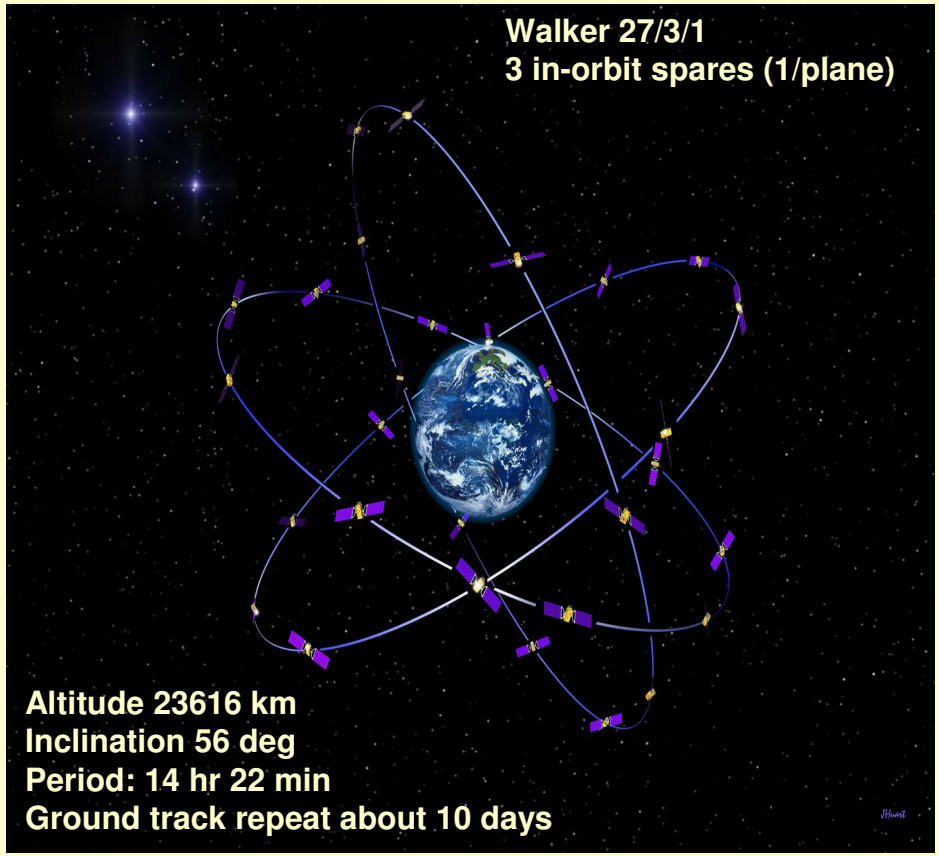
- Complex system distributed both in space and on ground.
- Safety includes both failure (RAMS) and fault free (Performance) scenarios
- High proportion of complex software
- Large and complex industrial organisation
- No identified certification authority.
- Multi-Modal System, providing SoL services to diverse users (aviation, maritime, rail etc.).

Safety Analysis

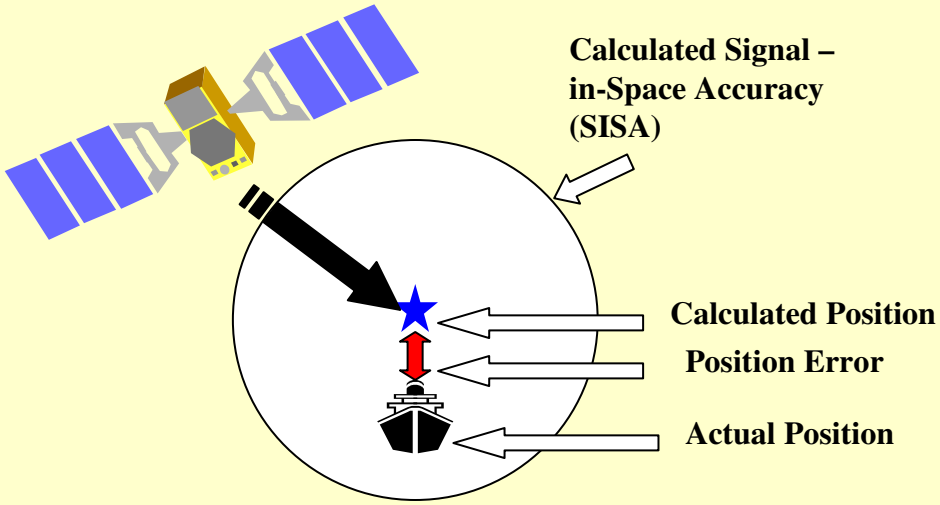
- Safety Analysis split into two areas
  - System in Fault Free mode
    - Analysis performed by System Engineering Performance team
    - Includes External Feared Events (iono, environment etc.) and Algorithm performance.
  - System in failed mode
    - Analysis performed by RAMS team
    - Includes HW and SW failures.

Safety& Dependability Design

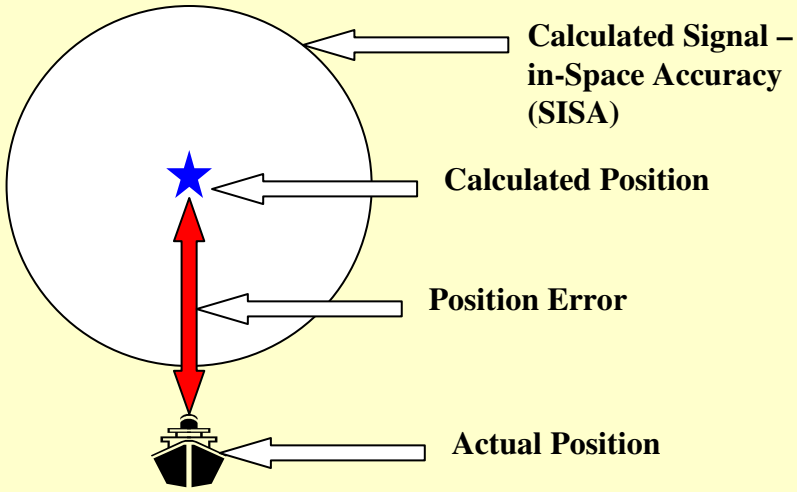
- Design greatly influenced by Performance & RAMS Requirements (Integrity, Continuity & Availability)
- Highlighted need for redundancy in Space & Ground Segments
- Functionally independent integrity (safety) chain



Integrity



OK - NO INTEGRITY EVENT



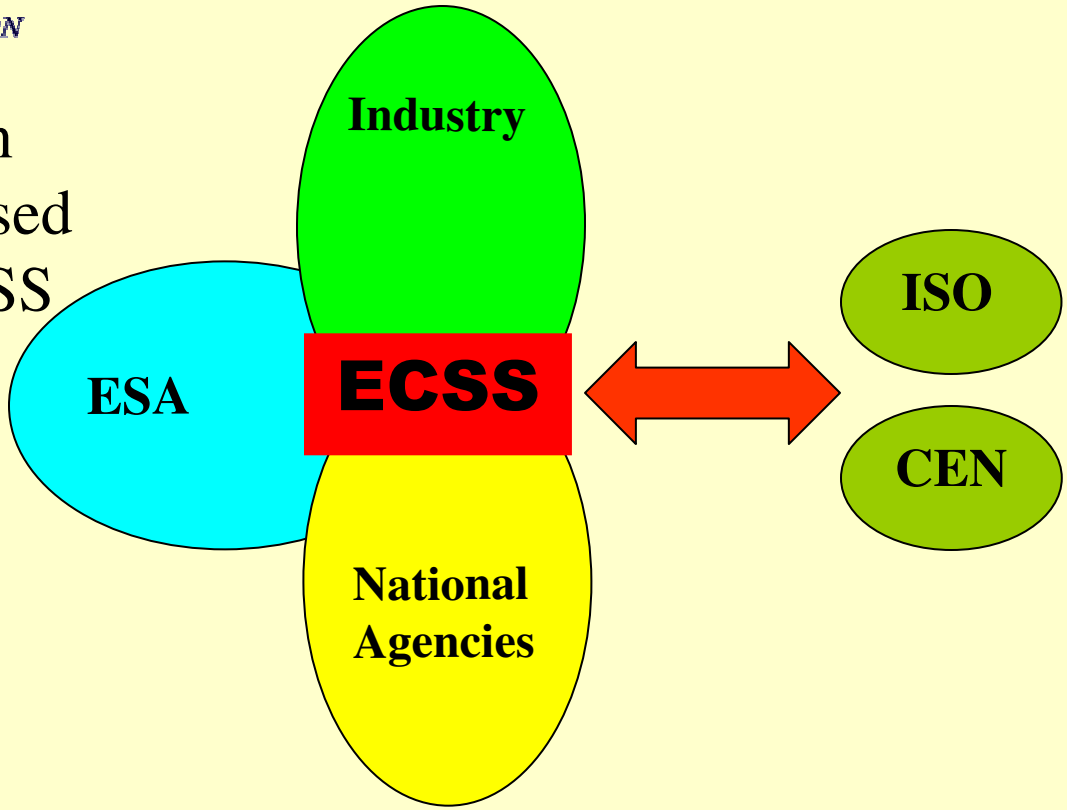
User not informed by System (Integrity Flag) within specified Time to Alarm

NOT OK - INTEGRITY EVENT

Standards

EUROPEAN COOPERATION
ECSS
FOR SPACE STANDARDIZATION

- System design based on recognised and accepted ECSS standards

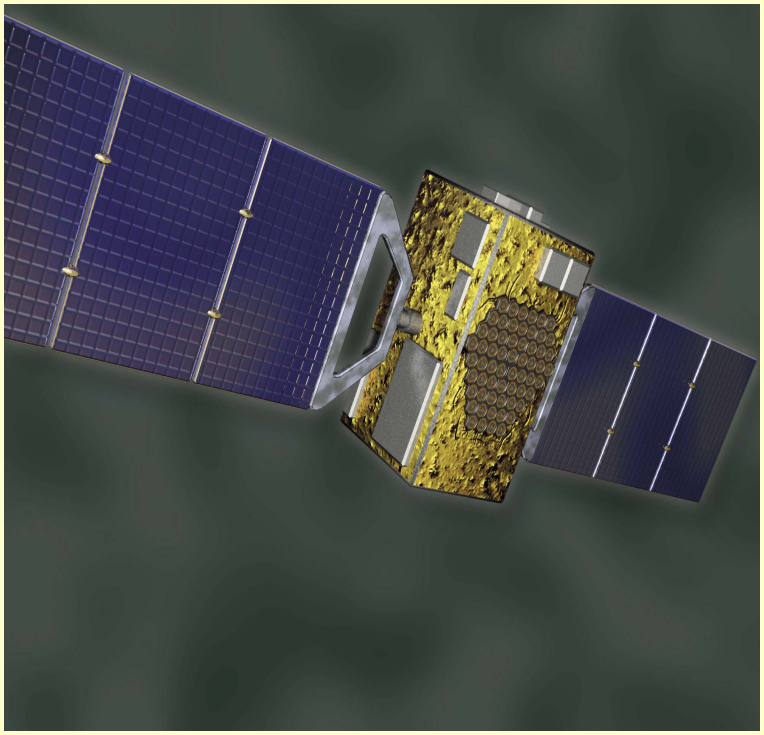


RAMS Analysis

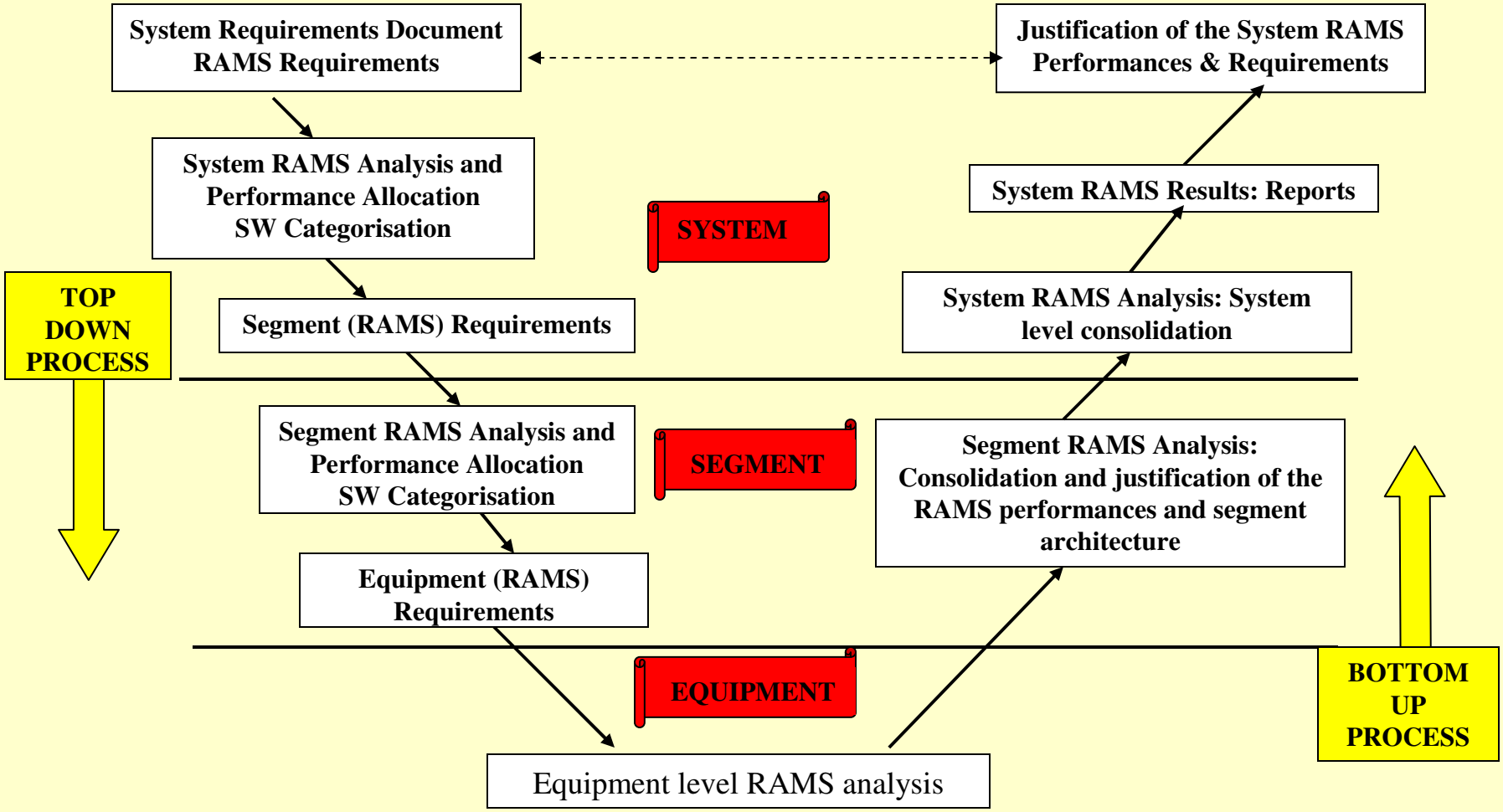
- RAMS Requirements applicable during different phases of the project
  - **Navigation Hazards** – affects the end users of the system.
  - **Classical Hazards** – affects the operators and maintainers of the system inc. launch site.
- Other safety requirements also included. (i.e Failure Tolerance)
- Comprehensive RAMS programme undertaken to verify requirements are achieved.
- SW addressed by allocation of Development Assurance Level (DAL) and then application of Galileo SW Standard

Safety Requirements

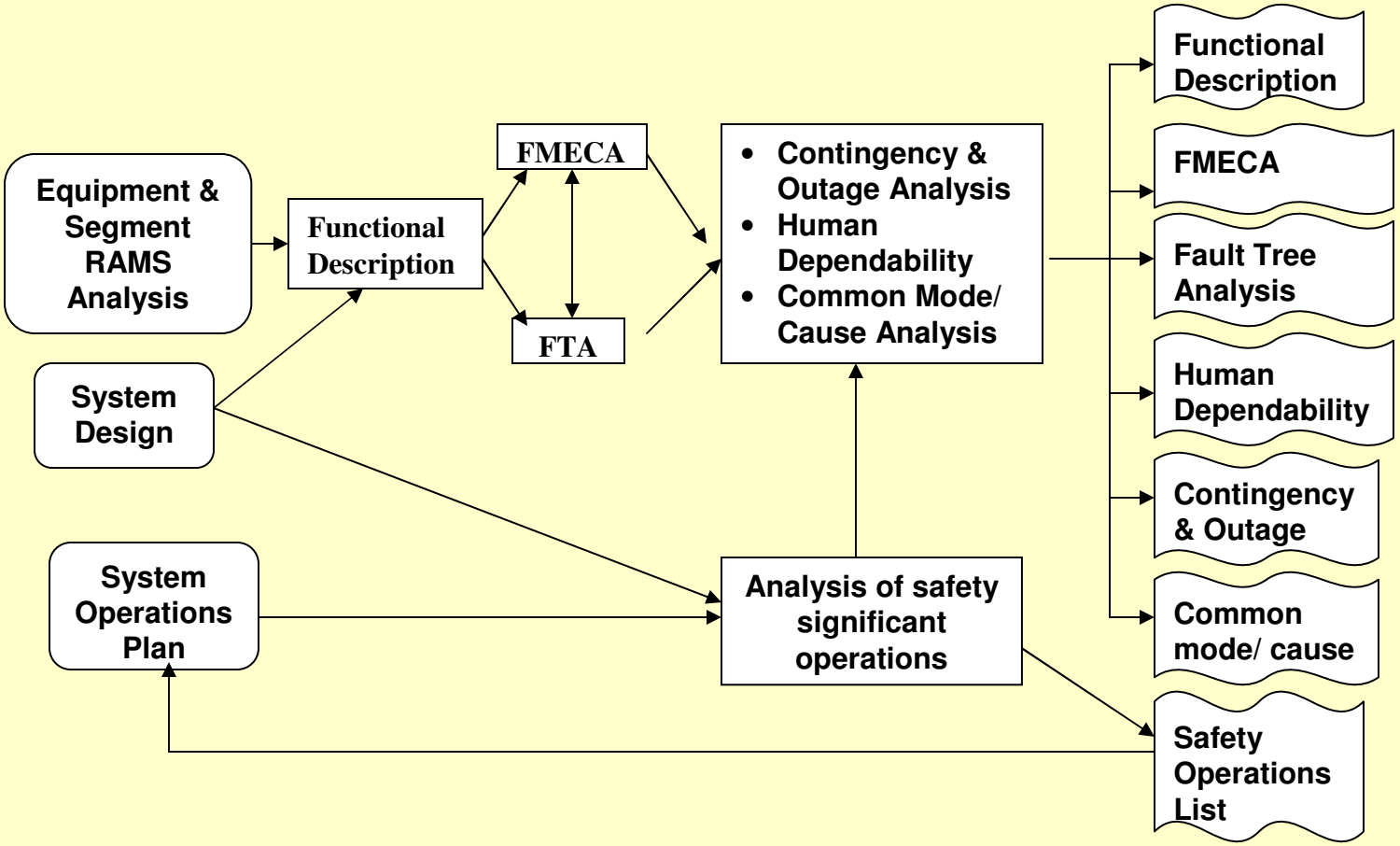
- Navigation Hazards – linked to Galileo Services
  - Driven by Integrity & Continuity requirements
  - Includes both fault free and faulty scenarios
  - Includes satellite control & maintenance operations
- Classical Hazards – linked to personal safety
  - Launch site safety
  - Personal hazards (operators & maintenance personnel, installation & testing).



RAMS Process



RAMS Studies



EGNOS Lessons Learnt

- EGNOS currently undergoing certification for SoL applications.
- Activity currently under the responsibility of GNSS Supervisory Authority in close collaboration with ESA and Civil Aviation.
- Safety case methodology adopted as method to achieve certification.
- Methodology comprises two parts:
  - System level: based on design, development and operations documentation
  - Application Level: tailored to the specific use of EGNOS (airports, harbours etc.)

Galileo Certification

- Applications using the Galileo Signal will have to be certified
- No certification requirements or Authority currently exist today.
- Maximum use made of lessons learnt from EGNOS certification.
- Need to assemble data to support certification .
- ESA already experienced in providing such analysis & documentation

Conclusion

- Galileo system to be used for safety critical applications.
- Design heavily influenced by dependability & safety requirements
- Comprehensive RAMS analysis undertaken to demonstrate RAMS requirements are satisfied
- No certification requirements or Authority are currently in place, however ESA must anticipate the need to provide data to support future certification
- Maximum use to be made of lessons learnt from current EGNOS certification activities
- ESA already experienced in providing such analysis and documentation however close interaction is to be maintained with certification entities